32 North Street
Portland Maine 04101
May 6, 2006

RECEIVED
2006 MAY -8 A 9:12
MAINE PUBLIC
UTIL. COMM.

Mr. Dennis Keschl
Acting Admininstrative Director
Maine Public Utilities Commission
242 State Street
Augusta, Maine 04330

Dear Mr. Keschl:

Enclosed is a Complaint, pursuant to §1302 of the Commission's statutes, requesting that the Commission investigate whether Verizon is coöperating, in Maine, with the National Security Agency's warrantless domestic wiretapping program.

Attached to the Complaint are two articles from the New York Times and the Los Angeles Times that describe NSA'a wiretapping program[1]; three e-mails to Verizon from my wife, Annie, and me on whether it is coöperating in Maine with the NSA program, and three e-mail replies from Mr. Drew Arena, a Verizon attorney; and the signatures, names, addresses, and phone numbers of the Complainants. The Complainants, who are all Verizon local exchange customers, received a copy of the Complaint, the newspaper articles, and the e-mail exchanges with Verizon, prior to signing the Complaint.

According to its e-mail responses, Verizon's position is that, because the NSA's domestic wiretapping program is "highly classified," federal laws prohibit them for discussing whether they are coöperating in Maine with that NSA program - even if they are not. As to whether Verizon has provided NSA access to its or MCI's switching facilities in Maine, Verizon states it is not aware of any statute that would prohibit it from doing so, but that, if it did, NSA would be prohibited from undertaking surveillance activities at those facilities by various laws, including the Foreign Intelligence Surveillance Act.

Two comments: Verizon being prohibited by federal law from saying whether it is coöperating in Maine with NSA's warrantless wiretapping activities, even if Verizon is *not* doing so, puts its customers in an Orwellian situation, which we hope the Commission can cut through. As for there being no federal or State of Maine statute that prohibits a telephone company, which is a Maine public utility, from providing a government agency such as NSA unwarranted access to its facilities: if that is true, the Commission obviously needs another statute; if it is not true, Verizon needs to be so advised, and immediately. But even if Verizon is correct on this point, we now know the president and the U.S. attorney general have declared that NSA does *not* have to comply with the FISA requirement that it obtain FISA Court orders prior to undertaking the wiretapping of U.S. citizens' calls and e-mails. So if indeed Verizon is providing NSA access to its facilities in Maine, Verizon is clearly wrong that NSA is prohibited from tapping calls to and from Verizon's customers in Maine.

The basis of our Complaint is the possibility that Verizon's e-mail responses reflect unreasonable utility practices, as referenced in §1302. The questions in our e-mails to Verizon are fundamental to the Complaint; namely, has Verizon provided NSA unwarranted access to call and

---

[1] I am attaching two recent Wired News pieces, which update and appear to validate these articles. One is about the first-hand experience of a former AT&T technician with the installation of NSA circuits in a 4ESS switch in AT&T's San Francisco central office; the other piece is the technician's affidavit. [Note: the 4ESS switch is a tandem switch, which routes calls from and to other companies' switches, and is similar to Verizon's tandem switch in Maine, to which all local and long distance carriers that do business in Maine are connected. Thus it is not surprising that NSA chose AT&T's tandem switch to collect call and e-mail records.]

Google Inc. et al v. Egger et al

Dockets.Justia.com

e-mail records of its customers in Maine, or to Verizon or MCI facilities in Maine? Thus, have circuits been installed in any Verizon or MCI facility in Maine that allow NSA to tap calls and e-mails, or have any of Verizon's or MCI's Maine customers' calls been included in data mining samples provided to NSA or directly sampled by NSA? Verizon's e-mail responses do not answer those questions; Complainants are relying on the Commission being able to use its statutory authority to get yes or no answers from Verizon.

Very truly yours,

JDCowie

James D. Cowie
Lead Complainant

P.S. In case it necessary for me to declare this: Until last January 31st, when I retired, I was a member of the Commission's technical staff for 18 years, most of which I worked on telephone cases, first as an expert witness on the Commission's advocate staff, and later on its advisory staff.

Whistle-Blower Outs NSA Spy Room

By Ryan Singel | Also by this reporter

AT&T provided National Security Agency eavesdroppers with full access to its customers' phone calls, and shunted its customers' internet traffic to data-mining equipment installed in a secret room in its San Francisco switching center, according to a former AT&T worker cooperating in the Electronic Frontier Foundation's lawsuit against the company.

Mark Klein, a retired AT&T communications technician, submitted an affidavit in support of the EFF's lawsuit this week. That class action lawsuit, filed in federal court in San Francisco last January, alleges that AT&T violated federal and state laws by surreptitiously allowing the government to monitor phone and internet communications of AT&T customers without warrants.

On Wednesday, the EFF asked the court to issue an injunction prohibiting AT&T from continuing the alleged wiretapping, and filed a number of documents under seal, including three AT&T documents that purportedly explain how the wiretapping system works.

According to a statement released by Klein's attorney, an NSA agent showed up at the San Francisco switching center in 2002 to interview a management-level technician for a special job. In January 2003, Klein observed a new room being built adjacent to the room housing AT&T's #4ESS switching equipment, which is responsible for routing long distance and international calls.

"I learned that the person whom the NSA interviewed for the secret job was the person working to install equipment in this room," Klein wrote. "The regular technician work force was not allowed in the room."

Klein's job eventually included connecting internet circuits to a splitting cabinet that led to the secret room. During the course of that work, he learned from a co-worker that similar cabinets were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego.

"While doing my job, I learned that fiber optic cables from the secret room were tapping into the Worldnet (AT&T's internet service) circuits by splitting off a portion of the light signal," Klein wrote.

The split circuits included traffic from peering links connecting to other internet backbone providers, meaning that AT&T was also diverting traffic routed from its network to or from other domestic and international providers, according to Klein's statement.

The secret room also included data-mining equipment called a Narus STA 6400, "known to be used particularly by government intelligence agencies because of its ability to sift through large amounts of data looking for preprogrammed targets," according to Klein's statement.

Narus, whose website touts AT&T as a client, sells software to help internet service providers and telecoms monitor and manage their networks, look for intrusions, and wiretap phone calls as mandated by federal law.

Klein said he came forward because he does not believe that the Bush administration is being truthful about the extent of its extrajudicial monitoring of Americans' communications.

"Despite what we are hearing, and considering the public track record of this administration, I simply do not believe their claims that the NSA's spying program is really limited to foreign communications or is otherwise consistent with the NSA's charter or with FISA," Klein's wrote. "And unlike the controversy over targeted wiretaps of individuals' phone calls, this potential spying appears to be applied wholesale to all sorts of internet communications of countless citizens."

After asking for a preview copy of the documents last week, the government did not object to the EFF filing the paper under seal, although the EFF asked the court Wednesday to make the documents public.

One of the documents is titled "Study Group 3, LGX/Splitter Wiring, San Francisco," and is dated 2002. The others are allegedly a design document instructing technicians how to wire up the taps, and a document that describes the equipment installed in the secret room.

In a letter to the EFF, AT&T objected to the filing of the documents in any manner, saying that they contain sensitive trade secrets and could be "could be used to 'hack' into the AT&T network, compromising its integrity."

According to court rules, AT&T has until Thursday to file a motion to keep the documents sealed. The government could also step in to the case and request that the documents not be made public, or even that the entire lawsuit be barred under the seldom-used State Secrets Privilege.

AT&T spokesman Walt Sharp declined to comment on the allegations, citing a company policy of not commenting on litigation or matters of national security, but did say that "AT&T follows all laws following requests for assistance from government authorities."

Ads by Google

Internet Phone
Unlimited calling for $19.99/month.
Savings of 36 to 66%! Start Today
www.CrossComWireless.com

Lorex Video Surveillance
View your current system from anywhere with the DVM2050
www.lorexcctv.com

Record Calls / Change CID
Record your calls. Change Caller ID Display. Cheap Rates/Great Service!
www.SpoofCard.com

Secret Stash Safes
Hide your money, jewelry or whatever else you don't want found!
www.SneakySafes.com

Wired News: Contact Us | Advertising | Subscribe
We are translated daily into Korean and Japanese

© Copyright 2006, Lycos, Inc. All Rights Reserved.
Your use of this website constitutes acceptance of the Lycos **Privacy Policy** and Terms & Conditions

Wiretap Whistleblower's Statement

By

Former AT&T technician Mark Klein has come forward to support the EFF's lawsuit against AT&T for its alleged complicity in the NSA's electronic surveillance. Here, Wired News publishes Klein's public statement in its entirety.

Full story: Ex-AT&T Worker Tells Of NSA Op

Statement: Mark Klein, April 6, 2006

My background:
For 22 and 1/2 years I worked as an AT&T technician, first in New York and then in California.

What I observed first-hand:
In 2002, when I was working in an AT&T office in San Francisco, the site manager told me to expect a visit from a National Security Agency agent, who was to interview a management-level technician for a special job. The agent came, and by chance I met him and directed him to the appropriate people.

In January 2003, I, along with others, toured the AT&T central office on Folsom Street in San Francisco -- actually three floors of an SBC building. There I saw a new room being built adjacent to the 4ESS switch room where the public's phone calls are routed. I learned that the person whom the NSA interviewed for the secret job was the person working to install equipment in this room. The regular technician work force was not allowed in the room.

In October 2003, the company transferred me to the San Francisco building to oversee the Worldnet Internet room, which included large routers, racks of modems for customers' dial-in services, and other equipment. I was responsible for troubleshooting problems on the fiber optic circuits and installing new circuits.

While doing my job, I learned that fiber optic cables from the secret room were tapping into the Worldnet circuits by splitting off a portion of the light signal. I saw this in a design document available to me, entitled "Study Group 3, LGX/Splitter Wiring, San Francisco" dated Dec. 10, 2002. I also saw design documents dated Jan. 13, 2004 and Jan. 24, 2003, which instructed technicians on connecting some of the already in-service circuits to the "splitter" cabinet, which diverts some of the light signal to the secret room. The circuits listed were the Peering Links, which connect Worldnet with other networks and hence the whole country, as well as the rest of the world.

One of the documents listed the equipment installed in the secret room, and this list included a Narus STA 6400, which is a "Semantic Traffic Analyzer". The Narus STA technology is known to be used particularly by government intelligence agencies because of its ability to sift through large amounts of data looking for preprogrammed targets. The company's advertising boasts that its technology "captures comprehensive customer usage data ... and transforms it into actionable information.... (It) provides complete visibility for all internet applications."

My job required me to connect new circuits to the "splitter" cabinet and get them up and running. While working on a particularly difficult one with a technician back East, I learned that other such "splitter" cabinets were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego.

What is the significance and why is it important to bring these facts to light? Based on my understanding of the connections and equipment at issue, it appears the NSA is capable of conducting what amounts to vacuum-cleaner surveillance of all the data crossing the internet -- whether that be peoples' e-mail, web surfing or any other data.

Given the public debate about the constitutionality of the Bush administration's spying on U.S. citizens without obtaining a FISA warrant, I think it is critical that this information be brought out into the open, and that the American people be told the truth about the extent of the administration's warrantless surveillance practices, particularly as it relates to the internet.

Despite what we are hearing, and considering the public track record of this administration, I simply do not believe their claims that the NSA's spying program is really limited to foreign communications or is otherwise consistent with the NSA's charter or with FISA. And unlike the controversy over targeted wiretaps of individuals' phone calls, this potential spying appears to be applied wholesale to all sorts of internet communications of countless citizens.

COMPLAINT AGAINST VERIZON
TO THE MAINE PUBLIC UTILITIES COMMISSION

Summary

This complaint is to request that the Commission investigate whether and to what extent Verizon has cooperated with the National Security Agency's warrantless domestic wiretapping program authorized by President Bush. Specifically, the complaint requests: [1] that the Commission determine whether Verizon has provided NSA, or any other government agency, unwarranted access to any Verizon or MCI facilities in Maine, or to records of domestic or international calls or e-mails made or received by their customers in Maine; and, should the Commission find Verizon has done so, [2] that the Commission determine whether Verizon has violated any Maine or federal statutes, and if it has, that Verizon be ordered to stop providing unwarranted access to its Maine facilities and customers' call and e-mail records.

Background

NSA's warrantless domestic wiretapping program was reported last December in the New York Times and the Los Angeles Times; two such articles are attached to this complaint. The LA Times article, in particular, mentions that AT&T installed in its switching machines a circuit designed by NSA to insure that law enforcement had access to phone calls, that AT&T provided the government with a database, code-named Daytona, which keeps track of phone numbers on both ends of calls as well as the duration of all land-line calls, and that the NSA has had a direct hookup into the database. Such a program is an example of "data mining," which is a statistical process aimed at detecting specific patterns in large samples of data, which the LA Times article said "can involve tracing potentially millions of innocent links to find a few suspicious ones." Thus to implement the data mining of large samples of telephone call and e-mail records, agencies such as NSA would have to obtain warrants under the Foreign Intelligence Surveillance Act for vast numbers of phone numbers and e-mail addresses, which, this article speculates, is why NSA is circumventing the FISA Court. NSA and the Justice Department have declared the program to be "highly classified" and have refused to discuss it with the intelligence and judiciary committees of Congress.

Verizon's Position

Attached are responses by Verizon to complainant questions about whether in its Maine operations it is cooperating with NSA's unwarranted domestic wiretapping program. The questions were sent to Verizon's president and chief executive officer, Ivan Seidenberg.[1]

---

[1] Verizon responses came not from Mr. Seidenberg but from Drew C. Arena, who in his response lists his Verizon title as Vice President and Associate General Counsel for Law Enforcement and National Security Compliance. Follow-up questions to Mr. Arena's responses were again sent to Mr. Seidenberg, and again responses came from Mr. Arena; therefore, subsequent questions were sent directly to Mr. Arena.

As to whether Verizon is cooperating with NSA in Maine, Mr. Arena's response states: "Based on public information, including the Attorney General's Congressional testimony, the NSA program …is highly classified as are the identities of any companies cooperating with the government. We accordingly cannot either confirm or deny cooperation in such a program." He also stated: "To the extent that we cooperate with government authorities, we are confident that we are complying with all applicable statutes."

Complainant follow-up questions asked Mr. Seidenberg to identify which "applicable" Maine and federal statutes Mr. Arena referred to, and, in particular, which statutes bind Verizon to treating as "highly classified" whether it is or is not cooperating in Maine with NSA, if in fact it is not. Mr. Seidenberg did not respond; Mr. Arena's response states: "The relevant federal laws are: the so-called Wiretap Act (18 USC sections 2510-2522), the Foreign Intelligence Surveillance Act, (50 USC Sections1801- 1871) the Electronic Communication Privacy Act (18 USC Sections 2701-2712) and the Communications Act (47 USC Sections 206-207, 222 and 605). In addition we comply with the applicable provisions of the Maine Revised Statutes, particularly Sections 709-713 of Title 15." As to the question: Why, if it is not cooperating in Maine with NSA's warrantless domestic wiretapping program, Verizon cannot say so, Mr. Arena states: "To the extent Verizon cooperates with authorities on intelligence-related matters, it is limited by federal criminal law in discussing any aspect of its activities, including whether there are activities at all. Section 798 of Title 18 of the U S Code makes it a crime to disclose any classified information 'concerning the communication intelligence activities of the United States.'"

Because Verizon's responses seemed to focus on statutes it complies with if it is cooperating in Maine with NSA's domestic wiretapping program, final complainant follow-up questions asked Mr. Arena to identify which of the federal and State of Maine statutes he cited prohibit Verizon from [1] releasing its subscribers' call records to a government agency such as the NSA without obtaining the subscribers' prior authorizations, and [2] providing a government agency such as the NSA access to its switching facilities in Maine; and that if none of the cited statutes prohibit Verizon from doing those things to identify which federal or State of Maine statutes do so. Mr. Arena's response regarding [1] states: "18 USC 2702 (a) (3) prohibits Verizon from 'knowingly divulging a record or other information pertaining to a subscriber to or customer of such service... to any governmental entity.' Subsection (c) of the same Section lists five exceptions permitting the disclosure of customer records to a governmental entity : (1) pursuant to the requirements of 18 USC 2703 (covering subpoenas, warrants court orders, and statutory authorizations); (2) with the consent of the customer; (3) as is necessary to the rendition of the service or the protection of the rights and property of the service provider; (4) in emergencies presenting danger of death or serious injury to any person; or (5) to the National Center for Missing and Abused Children in cases of child pornography." Regarding [2] (on providing NSA access toVerizon facilities in Maine), Mr. Arena states he is "not aware of any statute that would prohibit Verizon from allowing a governmental entity (or any third party for that matter) access to a Verizon facility. ...however, a government entity would still be prohibited from undertaking surveillance at that facility by the various laws I provided ...initially. I believe the closest provision which speaks directly to access to equipment is probably 18 USC Section 2701. It says 'whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this Section.'"[2]

Basis of the Complaint Against Verizon

Has Verizon provided NSA unwarranted access to call and e-mail records of its customers in Maine, or toVerizon or MCI facilities in Maine? Thus, have circuits been installed in any Verizon or MCI facility in Maine that allow NSA to tap calls and e-mails, or have any of Verizon's or MCI's Maine customers' calls been included in data mining samples provided to NSA or directly sampled by NSA? Verizon's responses to complainant questions do not answer those questions. The basis of this complaint is the possibility that Verizon's responses reflect unreasonable utility practices, as referenced in Section 1302 of the Commission's statutes. Accordingly, this complaint respectfully requests: [1] that the Commission determine whether Verizon has provided NSA, or any other government agency, unwarranted access to any Verizon or MCI facilities in Maine, or to records of domestic or international calls or e-mails made or received by their customers in Maine; and, should the Commission find Verizon has done so, [2] that the Commission determine whether Verizon has violated any Maine or federal statutes, and if it has, that Verizon be ordered to stop providing unwarranted access to its Maine facilities and customers' call and e-mail records.

---

[2] This response from Mr. Arena, which is attached, contains (probably inadvertently) an e-mail exchange with a colleague on how to answer the question on which statutes prevent Verizon from providing NSA access to its facilities in Maine, which includes the following remarks:
"not sure this answers second question – which is what law if any prohibits US from providing Gov't with access to facilitiy [sic]. I'm not sure that there is ANY statute like that . . . this wouldn't prohibit us from giving 'authorization'. The real issue is what the Govt would DO once it had 'access'. For instance, it would still be limited in its surveillance activities by Title III and FISA."
Note: Mr. Arena's response to this question did not mention that, should Verizon allow government access to its facilities, the government would be limited in its surveillance activities by Title III and FISA – possibly because the president has declared that NSA's domestic wiretapping program is *not* limited by FISA.